SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V11I7P117

Volume 11 Issue 7, 169-179, July 2024

Original Article

A Novel Direct, Indirect and Mutual Trust-Based Blockchain Modeling for Validation of Data Reliability in Integrated Edge Computing Environment

D. Jayakumar[1], K. Santhosh Kumar[2]

[1]*Department of Computer Science and Engineering, Annamalai University, Tamilnadu, India.*
[2]*Department of Information Technology, Annamalai University, Tamilnadu, India.*

Corresponding Author : jayakumarifetd@gmail.com

Received: 12 May 2024 Revised: 11 June 2024 Accepted: 11 July 2024 Published: 27 July 2024

Abstract *- The tremendous growth of the Internet of Things has led to a rapid increase in data. When there is voluminous data to be processed, the speed of data retrieval, response time, and storage becomes a huge problem. To solve this issue, the integration of edge computing and blockchain technology is proposed in this study. Edge computing and blockchain are two dominants reigning in the data world today. Their integration will eventually result in a paradigm shift from centralized data management to a more decentralized form. While integrating them, security and trust become a problem because, in edge computing, different nodes participate in the link, which may follow different protocols. To resolve this issue, authors propose two blockchain trust models, namely the direct and indirect trust-based blockchain model and the mutual trust chain-based blockchain model. The proposed models are evaluated against standard blockchain techniques like Bitcoin, Ethereum, and Hyperledger Fabric, and it has been proven that the proposed mutual trust chain algorithm outperforms all the other existing technologies. The performance metrics such as throughput, efficiency, packet delivery rate, execution time, delay, packet drop ratio, etc., are calculated under the introduction of attacks like interference and eavesdropping, malicious code injection, and sleep deprivation attacks to validate the reliability of data in an edge computing environment. The proposed algorithms have higher scalability, lower latency, and better efficiency.*

Keywords *- Blockchain, Trust, Edge computing, Data reliability, Internet of Things (IoT), Security attacks.*

1. Introduction

With the massive explosion of Internet of Things (IoT) devices everywhere, the amount of data being generated is believed to rise from 61% to 175% by the end of 2025 [1]. Processing all this data in centralized clouds will not be as feasible in the future as it is today. Hence, the concept of edge computing is introduced to deal with future data processing.

The aim of edge computing is not to eliminate the technology of cloud computing and the Internet of Things but rather to reduce the heavy, voluminous data that it deals with and share the burden of computation. As data keeps growing, one has to move forward toward next-generation techniques like 5G, edge computing, IoT, blockchain, distributed computing, etc.

Already having implemented the Internet of Things to a significant extent, it is high time now that one should concentrate on the development of techniques like edge computing and blockchain and perhaps even their integration. Combining two existing techniques to exploit their advantages is not new. For example, combining IoT with blockchain created a new area called Blockchain-based IoT (BIoT) and is found to have several advantages.

Similarly, integrating artificial Intelligence with edge computing results in edge intelligence, where artificial intelligence contains the necessary technologies and edge computing brings along the needed use cases and scenarios [2]. With the actual progress of 5G, the digital world will see more revolutions and cloud computing will be outdated then. Hence, there is a strong demand for the wide-scale integration of edge computing technologies along with blockchain, which will create a breakthrough in many fields.

1.1. Internet of Things (IoT)

IoT is a novel technique in which a device attached to anything and connected to the internet can produce data and stream it online. Induction of a wide variety of durable sensors that are of low cost, enhanced internet connectivity, technologies like cloud, Artificial Intelligence, deep learning, and big data have all contributed to the massive growth of IoT in today's world. IoT enables intercommunication among devices and networks. In the UN Conference on Climate Change (COP2) held in Paris in 2016 [3], it was decided that technology has the power to reduce carbon dioxide emissions through the introduction of smart objects in areas like smart waste management, smart cities, and intelligent homes [4].

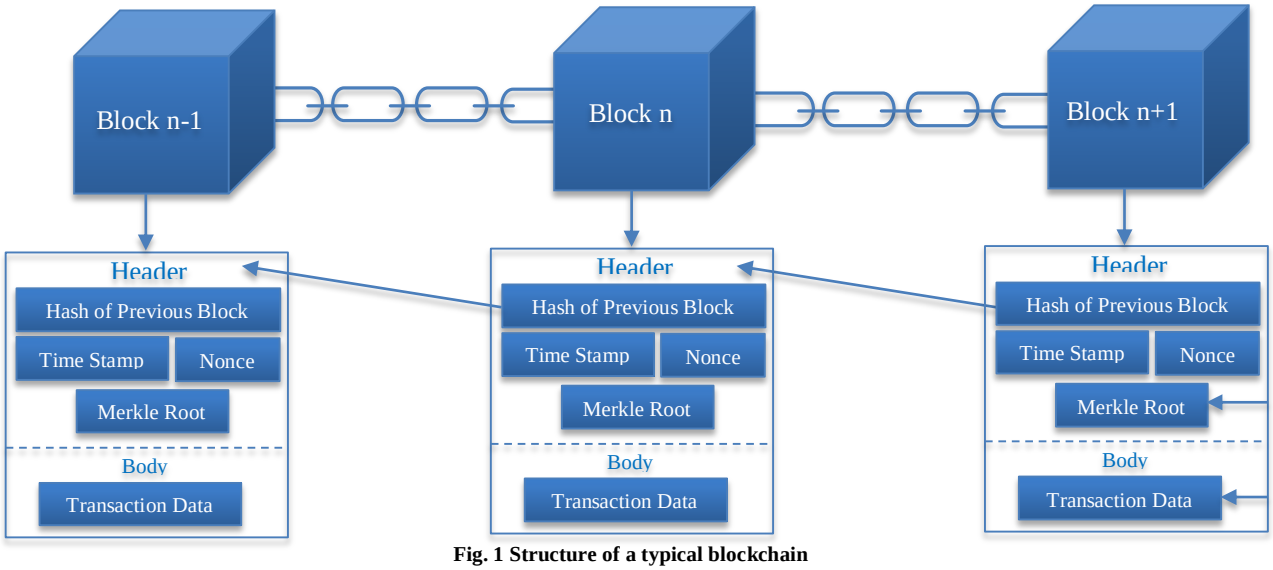

Fig. 1 Structure of a typical blockchain

1.2. Edge Computing

Edge Computing refers to the concept of distributed computing, which aims to move the process of computation towards the edge of the network as much as possible. The central idea behind it is to minimize the response time taken by the network and improve bandwidth utilization. It is a type of distributed computing that is location-sensitive [5, 6]. It is sometimes referred to as fog computing in certain cases. The evolution of edge computing started in the early 1990s. It is in contrast to cloud computing in the fact that cloud computing works on big data whereas edge computing acts on instant self data or local data. Though cloud computing serves to be successful in many aspects, it does not possess a quick rate of data transfer and retrieval time seems to be relatively low as well. Hence, it is proposed that edge computing will overcome the shortfalls of cloud computing and the Internet of Things.

1.3. Blockchain Technology

It is an advanced data storage methodology that is immutable and time-stamped [7]. Figure 1 shows the conceptual arrangement of blockchains. It consists of a distributed ledger, which is nothing but a database that stores transactions and smart contracts, which are self-executable sets of codes and some key cryptographic techniques.

There are three versions of blockchain, namely blockchain 1.0, which is a simple public ledger for cryptocurrencies. Blockchain 2.0 has come up with the usage of smart contracts for trust management and blockchain 3.0 is intended to be of use in a cloud platform [8]. Moreover, there are five types of blockchain namely public blockchain, private blockchain, consortium blockchain, permissioned blockchain, and hybrid blockchain. A public blockchain has no restrictions on reading data; everything is publicly available. In a private blockchain, there are some restrictions imposed and operations are carried out in a closed manner. A consortium blockchain is a type of blockchain where some nodes within the network are held responsible for the management of the blockchain itself. A permissioned blockchain is similar to a private blockchain but has certain read and write permissions that need to be obtained from the blockchain manager. Hybrid blockchain is a combination of both public and private blockchains. There is also something called sidechains, which are blocks that are not attached to the main blockchain but are run along with the main chain indicating that it is a subprocess.

There are three types of blocks called genesis blocks, which do not have any previous blocks. An orphan block is one whose parent block cannot be determined. Main blocks belong to the main chain, and side blocks belong to the side chains.

The working process of blockchain is explained here. The first step is to record the transaction. A transaction is defined as the movement of physical or digital assets from one node to another node in the blockchain. To record the transaction, one must know who does the transaction, what was passed in the transaction, when it was done, and why it was done. All these details are recorded in the transaction in the first step, and the next step is to gain consensus. Consensus is the process of obtaining permission from all the nodes that participate in the blockchain to validate the addition of the newly created block. Once the consensus is gained from all the parties, the created block is appended to the blockchain, and the corresponding hash value is attached to the created block for easy identification. The created block is then shared with all the nodes.

Each block consists of a header and body. The header consists of the index value, Merkle root, data, hash value, parent block, timestamp, and Nonce. Merkle tree is a new type of binary search tree where the nodes are connected through the hash pointers. Nonce stands for number used only once, which is a randomly generated number that is attached to the block. The body of the block contains the transaction counter, which contains all the transactions related to the block.

2. Literature Survey

The aim of the study by Guo et al. [9] is to create a consortium blockchain for data and log storage and to increase the hit ratio. The authors demonstrated that blockchain is one of the most promising trust-ensuring entities that has attracted many industries. The proposed algorithm is weighted to outperform existing ones in terms of hit ratio by 8 to 14% and 6 to 12% in delay average reported by the network.

Malik et al. [10] introduced a trust chain algorithm that has three layers such as data layer, blockchain layer, and application layer based on consortium blockchain. This algorithm is executed in a food supply chain scenario, the aim of which is to assign trust values dynamically to nodes participating in the network. A separate module is developed for calculating repetition scores of the nodes in the supply chain using its truthfulness value.

Mabodi et al. [11] proposed a system for recognizing grayhole attacks and achieved a detection rate of 94.5%. In a Grayhole attack, the attacker pretends to be the shortest path in the network and thereby prevents the data packets from reaching the destination which leads to loss of data. The proposed algorithm has four stages such as evaluating the trust of the nodes, verifying the rules, detecting grayhole attacks, and eradicating the attack.

Hammi et al. [12] proposed a virtual zone-based trust evaluation and identification process. The proposed work has been implemented in C++ language using Ethereum blockchain technology based on Sybil attacks and spoofing attacks. Here, the transactions are grouped into blocks, which are then verified using a consensus mechanism. Miners are verified and rewarded, and finally, blocks are added to the blockchain.

Christidis & Devetsikiotis [13] presented a survey of trust algorithms that are implemented in blockchain by evaluating underlying security and privacy. The attributes of trust chosen are active participation, service delivery, and attitude towards the service. The authors described trust in a digital platform as a key heuristic that is relied upon by the user.

Dorri et al. [14] proposed a local private blockchain that can be shared over networks. This strategy solved the identification problem. The main idea behind this is to build eight links for each action, which will overload the network in case of heavy IoT devices. Hardjono & Smith [15] proposed a privacy-preserving mechanism called the chain anchor method to make sure that users are paid for selling the data but still preserving privacy. The authors underlined the fact that major IoT devices often require identification.

Hashemi et al. [16] presented a novel method of smart device management with special identification of zones. This mechanism divides IoT space into zones like healthcare zones, home zones, etc., so that devices can be easily identified. If the zone wants to communicate with the blockchain, it must select a master that maintains a group identity for the zone and start communicating.

Cheng et al. [17] discussed the problem of double spending and its possible solutions in their study. Blockchain is a technology that has been of use in recent years in the field of cryptocurrency to make the concept of decentralization feasible. Blockchain techniques are using peer-to-peer networks. Authors recommended that, to avoid node failure, which may result in potential loss of information, an updated copy of the ledger must be made available to all the nodes in the blockchain.

Ben Amor et al. [18] suggested a blockchain-based solution that integrates blockchain and IoT for better device control. They also recommend considerable reconfiguration in the architecture of Ethereum. There are two types of keys, called private and public keys, for each device. To ensure safety and privacy, private keys belong to individual devices, and public keys to the entire blockchain network. Few researchers take on a new initialization to run an application safely on an untrustable network. This is made possible by remote attestation, which Trust Blogger does. It checks the hashtag using its unique ID and decides whether to trust it or not.

3. Proposed System

In this study, the authors propose two novel types of blockchain technology to estimate trust and validate data reliability at the edge servers. The two types of blockchain are direct and indirect trust-based blockchain and mutual trust chain-based blockchain model.

3.1. Trust

Trust in a digital platform refers to the measure of confidence that the user has towards the other party or the network. It is based on the behavior and capability of nodes that participate in the network. It is from the reliability factor measured by the trust that a node behaves in the future in terms of intended service and resource sharing. The properties of trust can be objective, subjective, and context-related in nature. There are three types of trust, namely data trust, privacy trust, and trust based on the entity.

Management of trust is a big deal that comprises of analysis of trust between devices before establishing a connection with them. The components of trust management are trust metrics evaluation like Quality of Service (QoS) and social trust. Once the trust has been evaluated, trust is formed based on the decision by the node, and trust scores are then propagated. The final step in trust management is to aggregate the trust information and update the trust values of each node. If the participants trust the blockchain as a whole, then no individual trust metric is needed, but due to the nature of the dispersal of nodes and their diverse characteristics, blockchain platforms become unsafe for data transmission without trust. Also, trust is a very important factor when establishing a relationship with the node in edge computing, as they are anonymous to each other and follow different protocols and levels of security.

Since the underlying cloud and IoT architectures are prone to several types of attacks, trust becomes an undeniable factor. Some of the well-known and common attacks are false data injection, malicious node injection, side-channel attacks, booting attacks, eavesdropping, denial of service attacks, Sybil attacks, spoofing attacks, node cloning, hardware failure, and cross-site scripting [19].

3.1.1. Components of Trust Management

Trust management involves a lot of entities like trust agents, trust extractors, trust lifecycle management modules, trust modeling algorithms, trust data, and trust information analysis.

Trust agent collects the trust data from the nodes in the network and evaluates it using trust information analysis and the estimated trust value is transmitted to other nodes for decision making. Managing trust in a cloud environment is hard because everything is virtualized, and nothing seems to be physically present for actual evaluation.

The three metrics based on which trust can be built are knowledge, experience, and reputation. For example, one may buy a product because one might have heard about it (Knowledge), or one might have used it earlier (Experience), or one might buy it just because of the popularity and belief that the particular brand has (Reputation). There are three types of trust used here namely direct trust, indirect trust, and mutual trust.

3.2. Direct Trust

Here, trust is calculated based on the connectivity of the node, its proximity, collaboration with others, prior experience of connecting with it, etc. It can be expressed using the following Equation (1).

$$d_r(u,v) = \frac{w(u,v)}{w(u)}, \text{where} d_r(u,v) \in (0,1] \tag{1}$$

Where w(u,v) signifies the trust strength between nodes, and w(u) represents the total strength between neighboring nodes. The performance metrics, such as attack detection time, drop ratio, and false positive rate, are calculated for the proposed algorithm.

3.3. Indirect Trust

Trust in this scenario refers to the flow of information between the concerned nodes. This type of trust is not directly made. Rather, an intermediary node that is adjacent refers to other nodes. This is called indirect trust. The algorithm for the direct and indirect trust model is given below. Equation (2) gives the formula for calculating indirect trust.

$$i_s(u,v) = \begin{cases} mt \dfrac{d_{\max} - d_{u,v} + 1}{d_{\max}} & if\ d_{u,v} \le d_{\max} \\ 0 & if\ d_{u,v} > d_{\max} \end{cases} \tag{2}$$

Where $mt = \min(d(u, u_1), d(u_1,u_2), \cdots, d(u_n,v))$, and d_{max} is the maximum trust transmission distance.

Direct and Indirect-based blockchain Algorithm:

Step 1 : Open transaction
Step 2 : Create blocks
Step 3 : Connect with neighbor blocks
Step 4 : Evaluate direct trust between blocks
Step 5 : Evaluate indirect trust between blocks
Step 6 : Form entire trust between blocks
Step 7 : If trust value meets the expected value, communication is established.

3.4. Mutual Trust

This is a combination of both direct and indirect trust. Closer nodes choose direct trust, and intermediary nodes use indirect trust. There is no central manager for carrying out this type of blockchain. It allows the usage of trust management services to elect Trustworthy Bloggers (TB). It contains two processes which are mining and consensus. Mining refers to the process of validating newly created blocks, and consensus is the process of collecting every node's agreement to add the new block to the chain. Consensus protocol is given below to execute the mutual trust chain-based blockchain algorithm. The participants of the consensus protocol are leaders, candidate trustworthy bloggers, nodes in the network, and trust service [20]. Mutual trust calculation is given in Equation (3).

$$m(u,v) = \begin{cases} min\big(T(u,v)\big) & \text{if } min\big(T(u,v)\big) \ge \chi \\ 0 & else \end{cases} \tag{3}$$

Where χ represents the trust tolerance degree.

Consensus Algorithm:

Step 1 : Trust service sends data for trust assessment
Step 2 : Trust is assessed
Step 3 : The leader is selected by nodes
Step 4 : Leader sends broadcast message
Step 5 : Find the prospective candidate list
Step 6 : Conduct voting on the candidate list
Step 7 : The leader selects trustworthy bloggers
Step 8 : Broadcast trustworthy bloggers
Step 9 : Nodes extract trust features for assessment
Step 10: Nodes send message and signature for validation
Step 11: Message is verified
Step 12: Candidate TBs broadcast votes for validation
Step 13: Leader adds or removes messages based on votes
Step 14: The leader broadcasts the decision made.

Miners are the ones who perform the task of mining. Trustworthy Bloggers (TB) are those who own the miners. TBs have a higher level of trust than other common nodes in the network. During consensus process execution, a voting process is done based on trust features. The collection of TBs is called TBpool (TBP). By implementing consensus protocol along with spinning and validation, TBP is enabled. Once it is enabled, the trust manager is chosen and this information is passed to all the nodes. They agree or disagree with this choice of election. If they agree, they

accept the sign created by the leader. The leader then, in turn, chooses the deputy bloggers.

The following are the benefits of integrating blockchain and edge computing technologies using the proposed model.

1. Moving from a centralized to a decentralized architecture.
2. Data and privacy loss prevention.
3. Improved security.
4. Reducing mega-scale cloud storage.
5. Reducing network traffic in IoT and cloud.
6. Efficient processing.
7. Reduced mining delay.
8. Better compatibility.
9. Enhanced privacy.

4. Result and Discussion

The two proposed algorithms are executed and the results have been simulated with a real-time IoT data-collecting device coupled with an AMD CPU of 32GB primary memory.

The performance metrics such as packet delivery rate, throughput, network delay, energy efficiency, packet drop ratio, encryption time, execution time, computational overhead, and storage cost are calculated for the proposed mutual trust chain algorithm and compared with existing blockchain technologies like Bitcoin, Ethereum, and Hyperledger Fabric.

The performance is measured under normal conditions and similarly when attacks like malicious code injection, sleep deprivation attack, interference, and eavesdropping attacks are artificially induced.

Table 1. Simulation parameters

Parameters	Value
Area	2500×2500 m^2
Time	400 s
Nodes	Normal: 50
Transmission Range	200 m
Mobility	Random mobility
Maximum Connections	100 nodes
Data Size	1024 bytes
Maximum Packet Speed	20 ms^{-1}

Bitcoin is a cryptocurrency-based blockchain technology that enables a digital payment system, and it works on public blockchain technology. It is open access and decentralized in form. Ethereum is also a public blockchain technology that provides cryptocurrency and uses smart contracts for execution. Smart contracts are self-executable sets of codes that are invoked when a predefined condition is met.

Hyperledger Fabric on the other hand, is also open source, but it is not a public blockchain. It is a format of permissioned blockchain owned by the Linux Foundation. It does not have cryptocurrencies associated with it. It uses the practical Byzantine Fault Tolerance method for making consensus.

Table 1 shows the simulation parameters that are used to execute the proposed system. Figure 2 displays the rate of packet drop that occurs when attacks on reentrancy and access control vulnerabilities are encountered

.

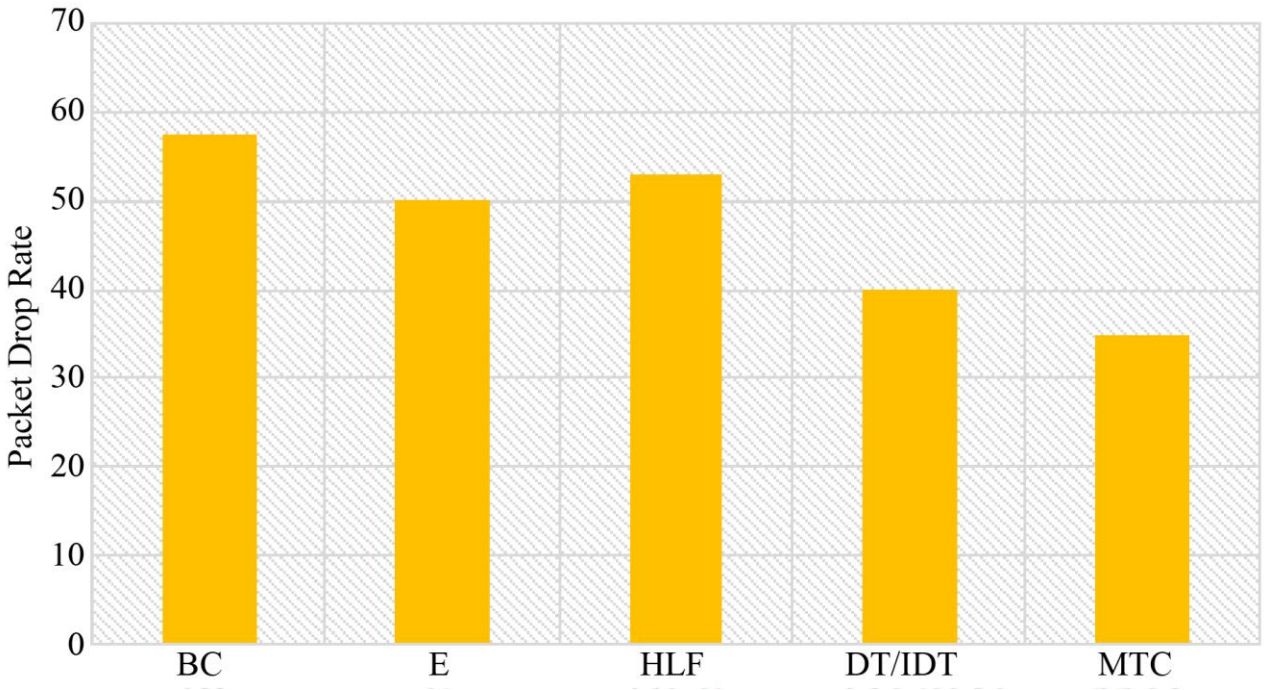

Fig. 2 Packet drop rate of algorithms

It has been found that the packet drop rate has been significantly reduced in the proposed models. Figure 3 shows the false positive rate that is associated with the proposed algorithm. The figure clearly shows the decrease in false positive rates. Figure 4 shows the detection time of wormhole attacks. The proposed models have a faster detection time when compared to other existing models. Figure 5 shows the packet delivery rate of existing and proposed algorithms. Figure 6 shows the throughput achieved by the algorithms. Figures 7 and 8 show the delay in network and energy efficiency of the existing and proposed mutual trust chain algorithm.

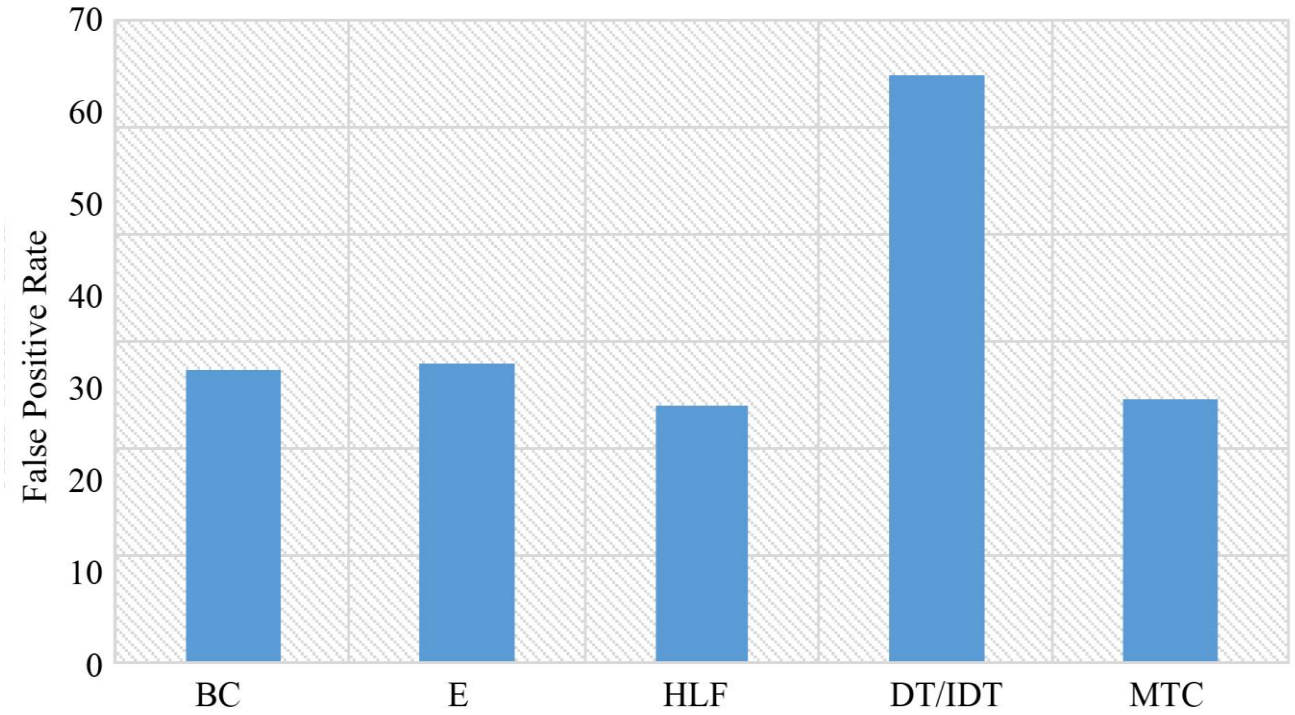

Fig. 3 False positive rate of algorithms

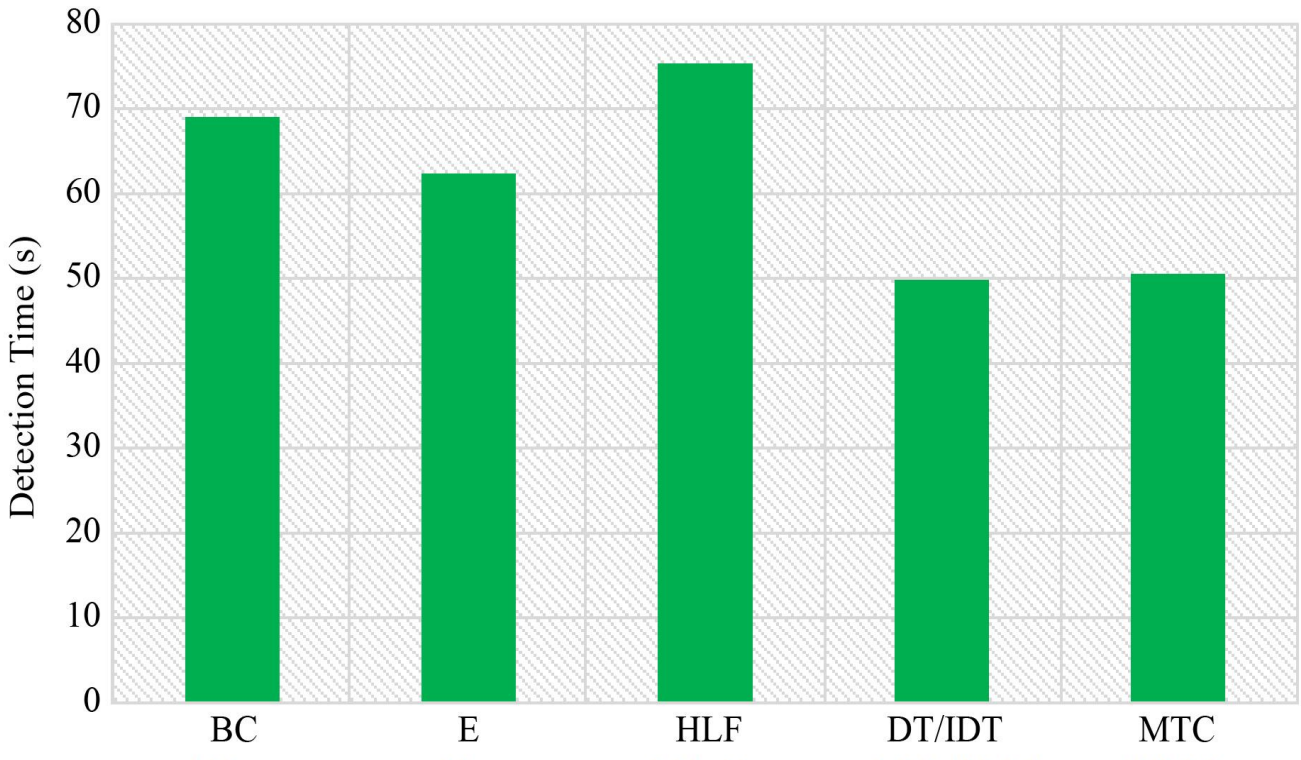

Fig. 4 Wormhole attack detection time

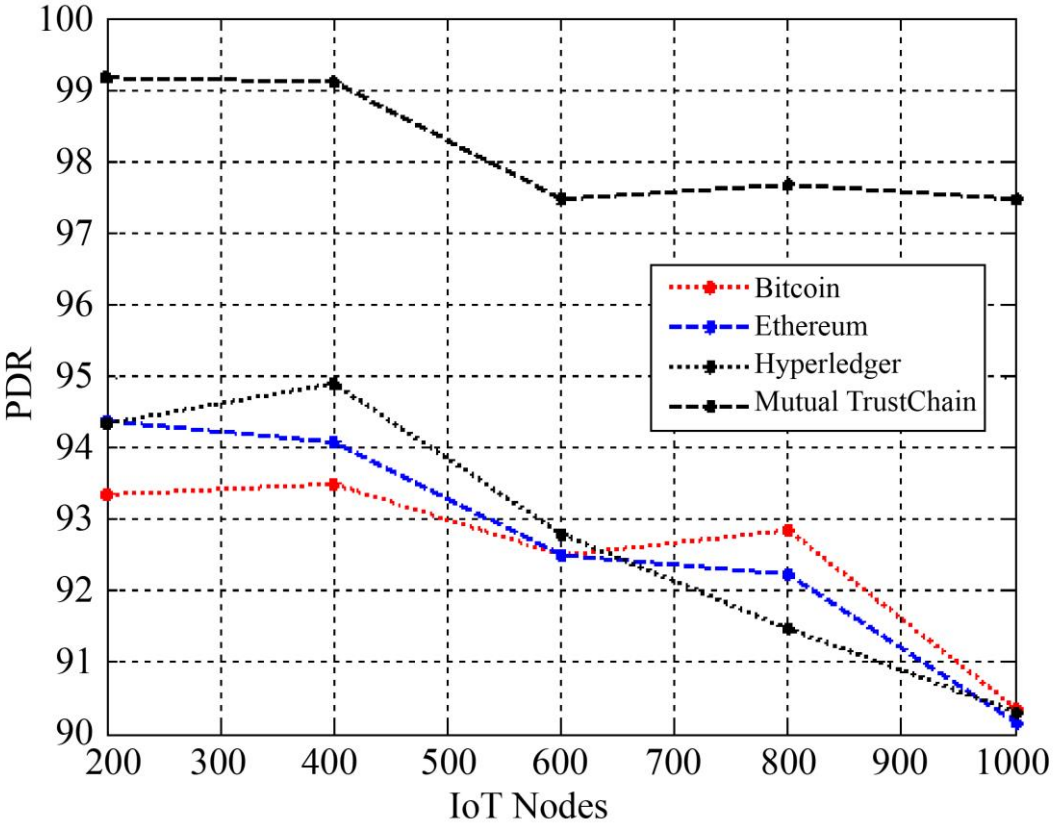

Fig. 5 Packet delivery rate

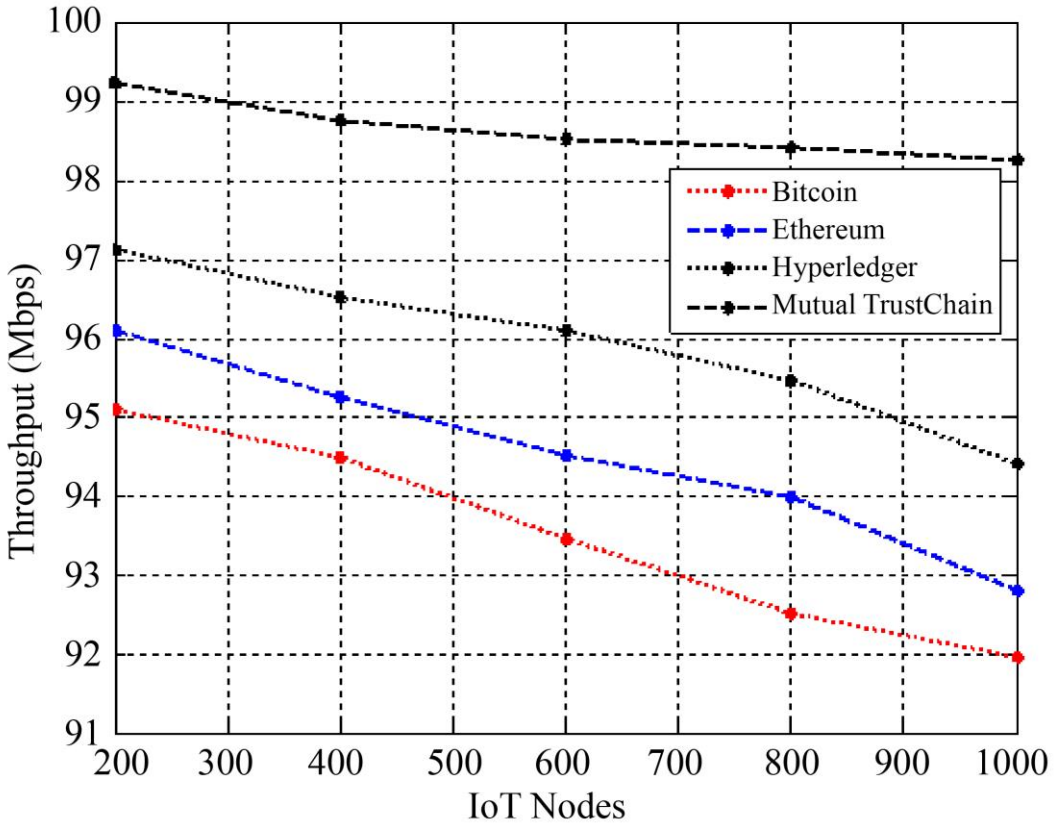

Fig. 6 Throughput

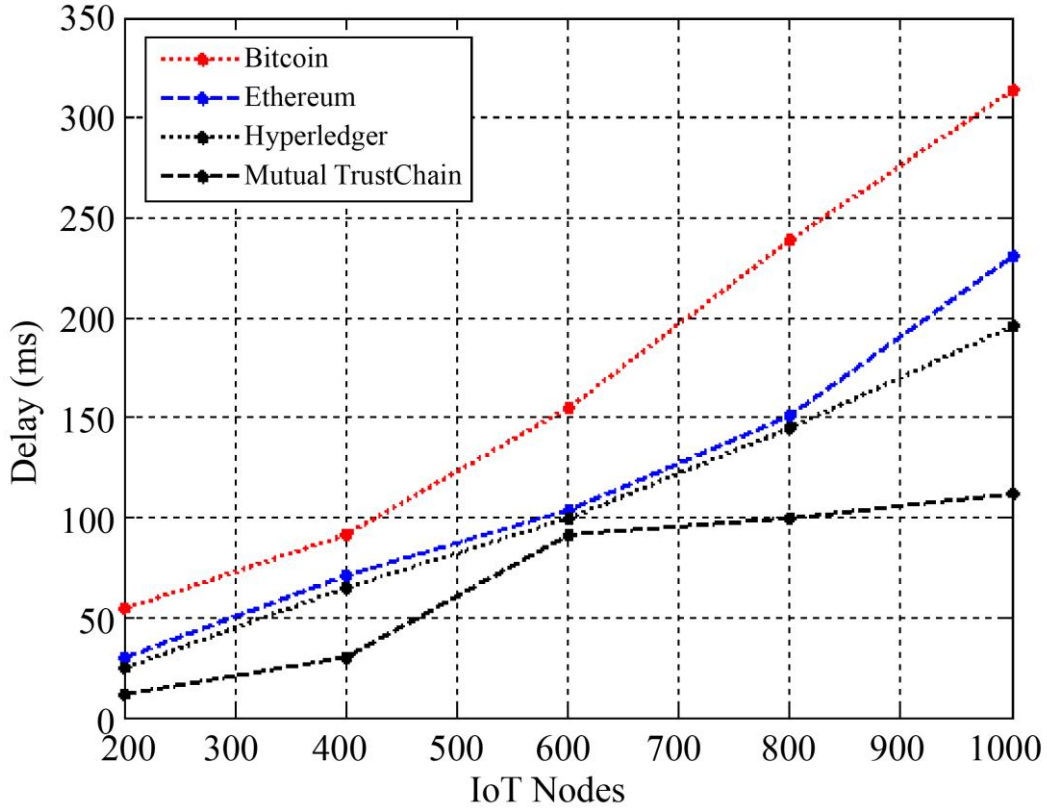

Fig. 7 Delay in network

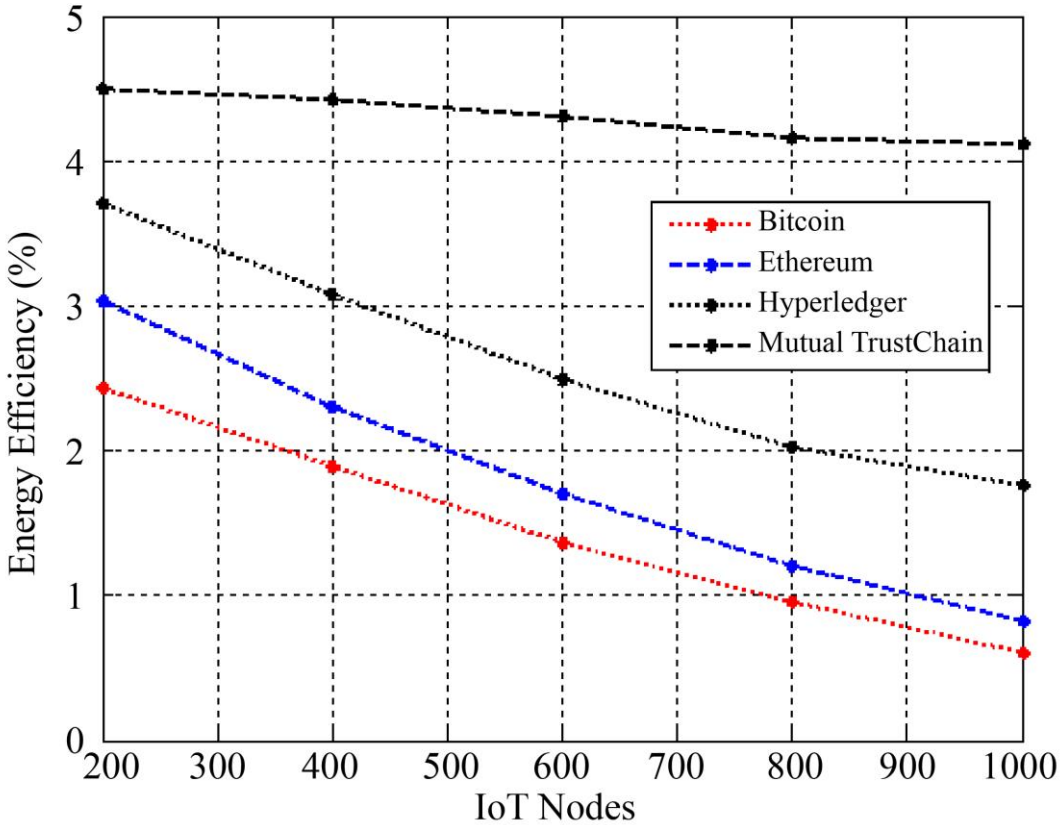

Fig. 8 Energy efficiency

Table 2. Performance under normal network conditions

Blockchain Models	Execution Time	Encryption Time	Storage Cost	Computational Overhead	Possibility of Packet Drops
Bitcoin	0.947	0.884	0.305	0.825	0.939
Ethereum	0.958	0.884	0.275	0.825	0.974
Hyperledger	0.960	0.9052	0.261	0.872	0.975
Proposed DT/IDT	0.965	0.9054	0.236	0.882	0.977
Proposed MTC	0.978	0.9155	0.230	0.902	0.983

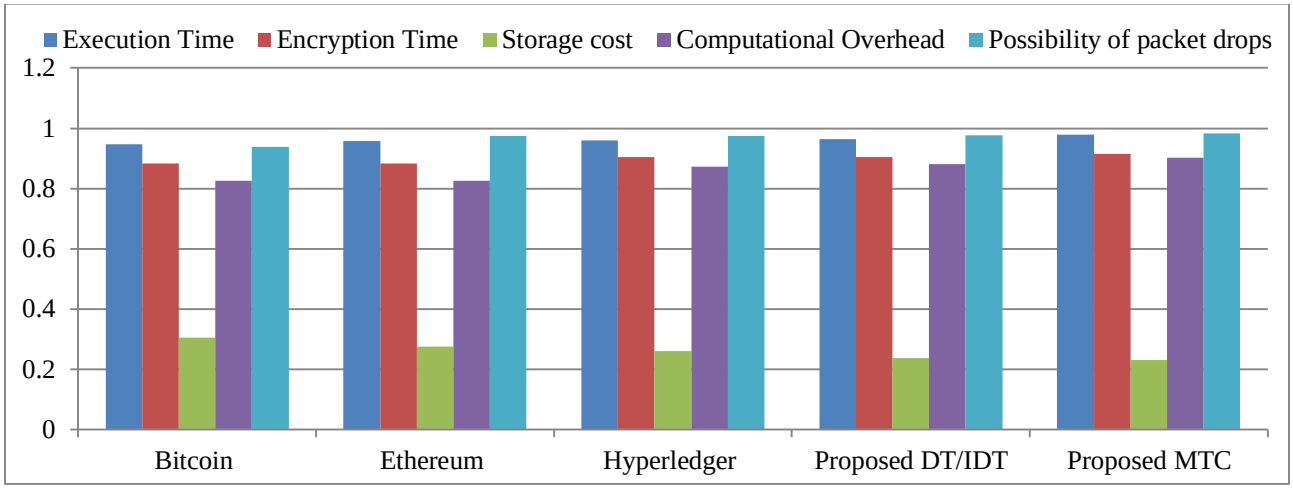

Fig. 9 Comparative analysis

Table 2 shows the execution time of the proposed and other existing models, encryption time, storage cost, and computational overhead under normal network conditions. Figure 9 shows the performance analysis of the algorithms under normal network conditions. Execution time, encryption time, storage cost, as well as computational overhead are shown in Table 3 when a malicious code injection attack is induced. Figure 10 shows the comparative analysis of the algorithms under malicious code injection attacks. Table 4 shows the behavior of the algorithms during a sleep deprivation attack.

Table 3. Performance under malicious code injection

Blockchain Models	Execution Time	Encryption Time	Storage Cost	Computational Overhead	Possibility of Packet Drops
Bitcoin	0.986	0.545	0.291	0.390	0.708
Ethereum	0.993	0.719	0.277	0.612	0.722
Hyperledger	0.993	0.722	0.249	0.736	0.750
Proposed DT/IDT	0.995	0.751	0.222	0.781	0.777
Proposed MTC	0.994	0.783	0.128	0.819	0.871

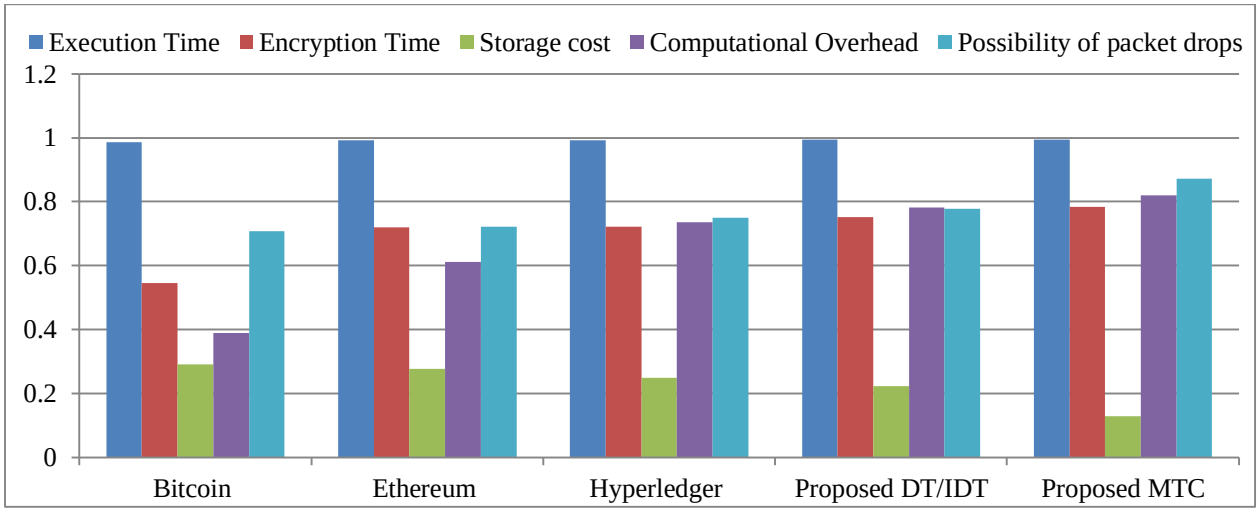

Fig. 10 Malicious code injection attack

Table 4. Performance under sleep deprivation attack

Blockchain Models	Execution Time	Encryption Time	Storage Cost	Computational Overhead	Possibility of Packet Drops
Bitcoin	0.995	0.880	0.0729	0.825	0.927
Ethereum	0.995	0.881	0.0729	0.826	0.927
Hyperledger	0.996	0.901	0.0649	0.869	0.935
Proposed DT/IDT	0.996	0.901	0.0635	0.869	0.9366
Proposed MTC	0.996	0.915	0.056	0.903	0.943

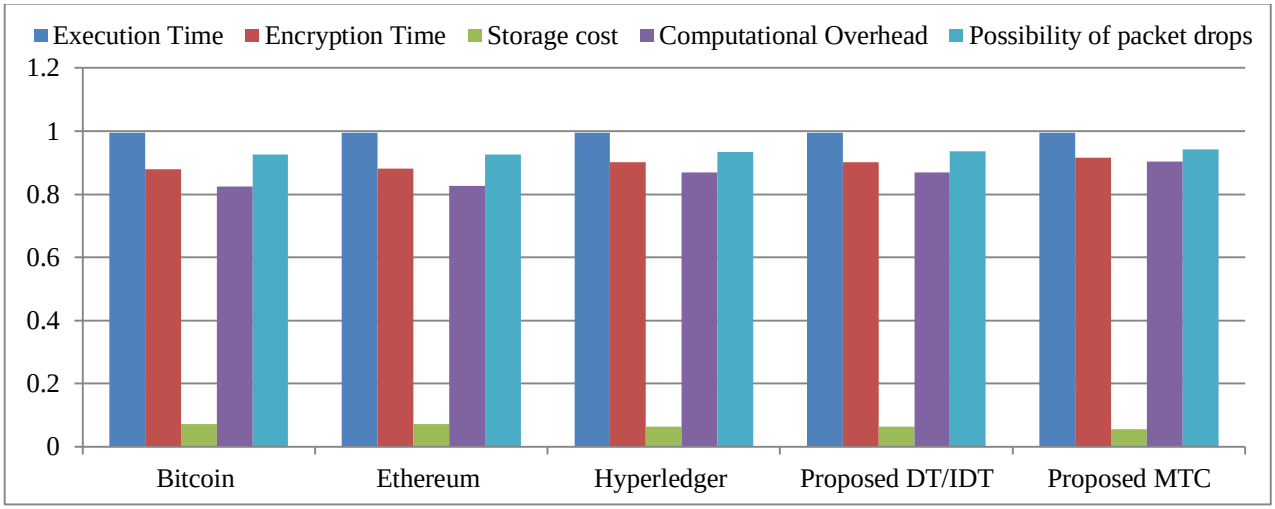

Fig. 11 Sleep deprivation attack

Table 5. Performance under eavesdropping attack

Blockchain Models	Execution Time	Encryption Time	Storage Cost	Computational Overhead	Possibility of Packet Drops
Bitcoin	0.998	0.913	0.088	0.849	0.911
Ethereum	0.999	0.928	0.083	0.881	0.977
Hyperledger	0.999	0.929	0.023	0.883	0.988
Proposed DT/IDT	0.999	0.934	0.022	0.883	0.994
Proposed MTC	0.999	0.936	0.011	0.894	0.997

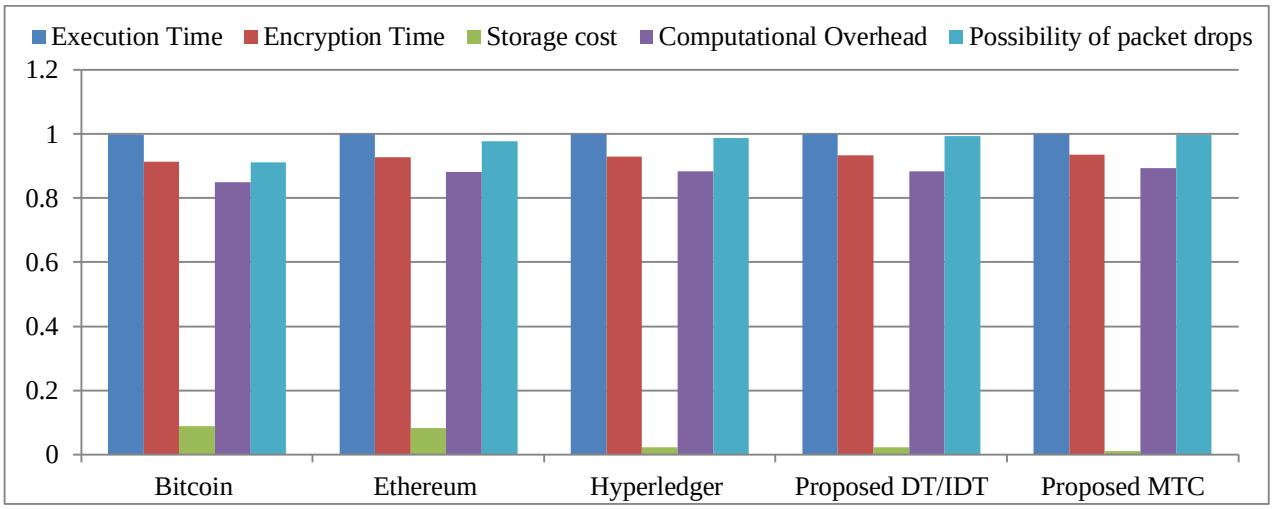

Fig. 12 Interference and eavesdropping attack

Figure 11 shows the comparative analysis of the algorithms under sleep deprivation attack. These metrics are likewise calculated when interference and eavesdropping attacks are conducted, as shown in Table 5. Figure 12 shows the comparative performance analysis of the algorithms under eavesdropping attack. It can be observed that in all the types of attacks, the two proposed algorithms outperform all the other existing blockchain technologies like Bitcoin, Ethereum, and Hyperledger. Between the two proposed algorithms, the mutual trust chain-based blockchain model performs slightly better than the direct and indirect trust-based blockchain model.

5. Conclusion

IoT networks, though very successful so far, suffer a lot of demerits because of their massive structure and device ubiquitous nature. They do not provide a safe platform for communication and data transfer.

Therefore, to overcome these security issues, this study proposes novel models to make a shift to decentralized operations with the integration of edge computing and blockchain technologies. Two novel blockchain algorithms based on trust that perform better than existing blockchain technologies like Ethereum, Bitcoin, and Hyperledger Fabric are presented. The performance indices, such as packet drop rate, efficiency, execution time, throughput, attack detection time, etc., are calculated.

The two proposed algorithms yielded better outcomes when various attacks like malicious code injection, sleep deprivation attacks, interference, and eavesdropping attacks were artificially introduced. In the future, this study can be further extended to address the problems of identity concealment and content concealment.

References

[1] Qurat-ul-Ain Arshad et al., "Blockchain-Based Decentralized Trust Management in IoT: Systems, Requirements and Challenges," *Complex & Intelligent Systems*, vol. 9, no. 6, pp. 6155-6176, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[2] Davide Ferraris et al., "A Survey on IoT Trust Model Frameworks," *The Journal of Supercomputing*, vol. 80, no. 6, pp. 8259–8296, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[3] Wenjuan Li et al., "Blockchain-Based Trust Management in Cloud Computing Systems: A Taxonomy, Review and Future Directions," *Journal of Cloud Computing*, vol. 10, no. 1, pp. 1-34, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[4] Seyoung Huh, Sangrae Cho, and Soohyung Kim, "Managing IoT Devices Using Blockchain Platform," *2017 19th International Conference on Advanced Communication Technology*, PyeongChang, Korea (South), pp. 464-467, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[5] Simon Johnson et al., "*Intel Software Guard Extensions: EPID Provisioning and Attestation Services*," White Paper, vol. 1, pp. 1-10, 2016. [Google Scholar] [Publisher Link]

[6] A.S.M. Kayes et al., "Achieving Security Scalability and Flexibility Using Fog-Based Context-Aware Access Control," *Future Generation Computer Systems*, vol. 107, pp. 307-323, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[7] Abduljaleel Al-Hasnawi, Steven M. Carr, and Ajay Gupta, "Fog-Based Local and Remote Policy Enforcement for Preserving Data Privacy in the Internet of Things," *Internet of Things*, vol. 7, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[8] Arwa Alrawais et al., "An Attribute-Based Encryption Scheme to Secure Fog Communications," *IEEE Access*, vol. 5, pp. 9131-9138, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[9] Shaoyong Guo et al., "Blockchain Meets Edge Computing: A Distributed and Trusted Authentication System," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 1972-1983, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[10] Sidra Malik et al., "Trustchain: Trust Management in Blockchain and IoT Supported Supply Chains," *2019 IEEE International Conference on Blockchain*, Atlanta, GA, USA, pp. 184-193, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[11] Kobra Mabodi et al., "Multi-Level Trust-Based Intelligence Schema for Securing of Internet of Things (IoT) Against Security Threats Using Cryptographic Authentication," *The Journal of Supercomputing*, vol. 76, pp. 7081-7106, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[12] Mohamed Tahar Hammi et al., "Bubbles of Trust: A Decentralized Blockchain-Based Authentication System for IoT," *Computers & Security*, vol. 78, pp. 126-142, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[13] Konstantinos Christidis, and Michael Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292-2303, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[14] Ali Dorri, Salil S. Kanhere, and Raja Jurdak, "Towards an Optimized Blockchain for IoT," *2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation*, Pittsburgh, PA, USA, pp. 173-178, 2017. [Google Scholar] [Publisher Link]

[15] Thomas Hardjono, and Ned Smith, "Cloud-Based Commissioning of Constrained Devices Using Permissioned Blockchains," *Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security*, Xi'an China, pp. 29-36, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[16] Sayed Hadi Hashemi et al., "World of Empowered IoT Users," *2016 IEEE First International Conference on Internet-of-Things Design and Implementation*, Berlin, Germany, pp. 13-24, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[17] Lichen Cheng et al., "Account Guarantee Scheme: Making Anonymous Accounts Supervised in Blockchain," *ACM Transactions on Internet Technology*, vol. 21, no. 1, pp. 1-19, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[18] Ben Amor, Mohamed Abid, and Aref Meddeb, "CASK: Conditional Authentication and Session Key Establishment in Fog-assisted Social IoT Network," *2019 15th International Wireless Communications & Mobile Computing Conference*, Tangier, Morocco, pp. 114-119, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[19] Chirag Modi et al., "A Survey of Intrusion Detection Techniques in Cloud," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 42-57, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[20] Cong Zuo et al., "CCA-Secure ABE with Outsourced Decryption for Fog Computing," *Future Generation Computer Systems*, vol. 78, no. 2, pp. 730–738, 2018. [CrossRef] [Google Scholar] [Publisher Link]